运动控制产品

应用说明文档
机械安全

AN00209

版本 D（中文）

本文件仅作为说明性指南，不作为担保机器制造商完全满足相关安全要求的程序。机器制造商有完全责任遵守所有相关标准和安全法规。

简介

本应用说明文档旨在向机器制造商提供有关功能安全以及如何在 ABB 运动产品中实施功能安全的指南。本应用说明文档提供有关功能安全的背景信息。

本应用说明文档与主要详细说明如何安全地使 ABB 运动产品的伺服驱动停止运行的附加应用说明文档相关：

AN00206 - 在 ABB 伺服驱动上实施安全功能

机器制造商的法律义务

欧盟目前在协调所有成员国的安全法规。希望向欧洲销售设备的机器制造商需遵守这些法规。这些法规与全球其他地区的安全法规有许多类似之处。

CE 认证与功能安全：

如果制造商用 CE 认证标志标记某产品，则表示该产品符合所有相关欧洲指令。机械指令中的机器定义如下：

- 由相互连接的零部件为特定用途组装成的组件，其中至少有一个零部件是可以运动的
- 机器或复杂工厂组成的组件（复杂工厂包含生产线与由多个机器组成的专用机械）
- 安全部件，例如：光幕、安全垫等
- 可变更机器基本功能的可互换设备

机器制造商指组装机器或任何机器零件的人士，还包装改装机器的机器用户或创建组件（例如：多台机器的生产线）的最终用户。机器制造商为自身目的制造的机械同样须符合这些法规。

满足机械指令中基本健康和安全要求（EHSR）的过程可分为9个独立的步骤。本应用说明文档的后续内容进一步详细描述了这些步骤：

1. 管理功能安全
2. 评估风险
3. 降低风险
4. 制定安全要求
5. 实施功能安全系统
6. 验证功能安全系统
7. 确认功能安全系统
8. 形成文件
9. 合规

机器指令与安全部件：

在机械指令中，安全部件的描述如下：
- 用于满足安全功能
- 在市场上独立出售
- 失效和/或故障会危及接触人员的安全
- 对于机械功能而言不必要，或为使机械运作，可由普通部件替代。

通常会影响ABB运动产品运行过程的电气安全部件包括：
- 专门设计用于检测人员，以确保人员安全的电敏感设备，例如：非材料屏障、传感器垫、电磁检测器
- 可运动的电动保护开关
- 急停装置
- 超速限制装置
- 电气安全装置，即含电子部件的安全开关

机器标准：

机械指令列举了 600 多种被协调的标准，还有更多未被协调的标准。以下简要列举了与在机器中使用的电子驱动相关的主要通用标准。这些标准中的许多专用于特定类型的机器，称为 C 标准。如果无可用相关 C 标准，则使用通用标准。以下列举了本应用说明文档中讨论的标准。

EN ISO 13849-1:2008协调标准

机械安全-控制系统的相关部件-第1部分：设计通则 -EN ISO 13849-1是通用功能安全标准，为欧盟内的符合性提供了参考，涵盖机械的电气、电子、可编程电子、机械、气动和液压安全。
EN 62061:2005协调标准。机械安全性-与安全有关的电气、电子和可编程电子控制系统的功能安全

EN ISO 14121-1:2007协调标准

机械安全-危险评估-第1部分：原理

第 1 步：管理功能安全：

为实现要求的功能安全级别，首先需正确管理功能安全，这可通过安全计划实现。安全计划执行以下功能：

- 识别所有相关活动。
- 描述功能安全的实施政策和策略。
- 识别责任。
- 确定形成文件的程序与使用的资源。
- 描述安全体系设置的管理。
- 包含验证与确认计划。

第 2 步： 评估风险：

该过程识别与评估与机器相关的每种风险。理想上，应通过设计变更排除评估出的高风险。如不可能，可通过实施安全功能降低风险。作为最后的手段，应将剩余风险明确地记在用户手册中。应在机器上固定清晰的标记，以警示机器上存在的危险。

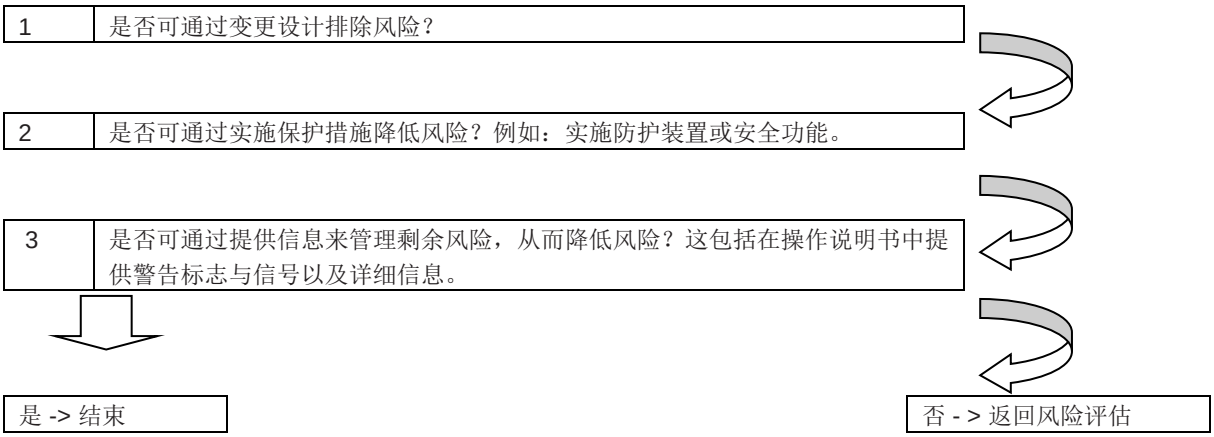
EN ISO 14121-1:2007 和 EN ISO 12100-1:2003 标准解释了风险分析与风险最小化过程。这两项标准中有许多重复部分，但基本风险评估程序包含以下步骤：

第 1 步	确定机器的限制与预期用途。这些限制可分为以下类别： – 使用限制 – 空间限制 – 环境限制 – 生命周期与使用寿命限制 – 其它限制
第 2 步	识别与机器相关的危害。
第 3 步	逐一评估识别出的风险。风险级别是以下两个属性值的乘积：风险的*严重程度*与风险的发生概率。
第 4 步	评估风险级别。风险级别是否足够低？
是 -> 结束	否 -> 降低风险

分别记录各危害的评估过程。如果分析结果显示风险可接受，则结束评估过程。如果风险仍不可接受，则执行第 3 步。

第 3 步：降低风险：

EN ISO 12100-1 推荐了 3 个用于降低无法排除的风险的步骤。



肯定会剩余无法通过技术或设计变更进一步降低的风险，须在操作说明书中记录这些风险。文件中可建议进一步降险措施，包括：

- 引入安全作业程序
- 监督作业过程
- 采用作业许可体系
- 使用个人防护设备
- 培训用户

本应用说明文档中的剩余步骤进一步详述了如何实施安全功能（降险程序的第2个选项）。

第 4 步：制定安全要求：

上述降险过程尝试将所有风险降至可接受的级别。为进一步降低风险，难免会需要某类安全功能。安全功能降低在接触危险时发生事故的概率。安全功能并非机器正常运行的一部分，即使安全功能失效，机器仍可运行。须评估安全功能对识别出的每一种危害的防护性能。

安全功能包括措施（用于降低风险）与安全性能（对措施有效性的衡量）。例如，如果危险由旋转轴造成，则措施可能是在安全门打开后的一秒内使电机停止运转。

随后需确定必要的安全性能。为此，可参考两项标准，这两项标准采用不同的方法。一项是 EN 62061 标准，该标准确定安全功能的安全完整性级别（SIL）。另一项是 EN ISO 13849-1 标准，该标准确定性能级别（PL）。这两项标准等效，可使用任意一种。

具体应根据技术、经验与用户要求进行选择。EN62061 更适用于控制系统，而 EN ISO 13849-1 则更为通用。

确定必要的 SIL （EN62061）

以下列举了确定 SIL 的步骤：

1. 确定危险造成的后果的严重程度。
2. 确定可能的危险接触频率与时间。
3. 确定接触危险后发生危险事件的概率。
4. 确定避免危害的可能性。
5. 详见下表。
6. 频率（Fr）、发生概率（Pr）与避免危害的可能性（Av）之和决定级别（Cl）。
7. 级别与危险程度（Se）决定必要的 SIL。

危害的发生概率					
Fr		**Pr**		**Av**	
频率、时间		**危险事件的发生概率**		**避免**	
<=1 小时	**5**	很高	**5**		
> 1 小时 <= 1 天	**4**	很可能	**4**		
> 1 天 <= 2 周	**3**	可能	**3**	不可能	**5**
> 2 周 <= 1 年	**2**	很少	**2**	可能	**3**
>1 年	**1**	可忽略	**1**	很可能	**1**

危害的严重程度	
Se	
后果（严重程度）	
死亡、失去一只眼睛或一只胳膊	4
永久失去手指	3
可医治	2
可急救	1

SIL 级别				
级别（CL）				
3-4	5-7	8-10	11-13	14-15
SIL2	SIL2	SIL2	SIL3	SIL3
OM	OM	SIL1	SIL2	SIL3
OM	OM	OM	OM	SIL1
OM=其它措施				OM

在上表标黄的示例中，**Cl = Fr + Pr + Av** = 5 + 3 + 3 = 11。**Se**=3，因此 **SIL 为 2 级**。

确定必要的 PL （ISO13849-1）

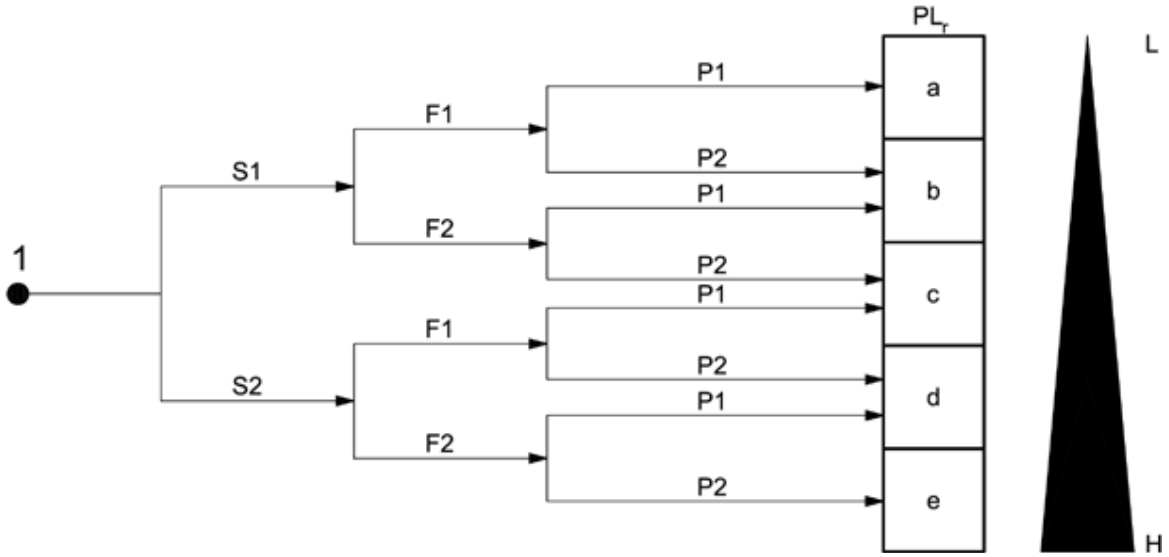
以下列举了确定 PL 的步骤：

1. 确定损害的严重程度。
   S1 表示可逆的轻伤。
   S2 表示不可逆的重伤或死亡。

2. 确定与危险接触的频率和时间。
   F1 表示极其频繁地或短时间接触
   F2 表示连续或长时间接触

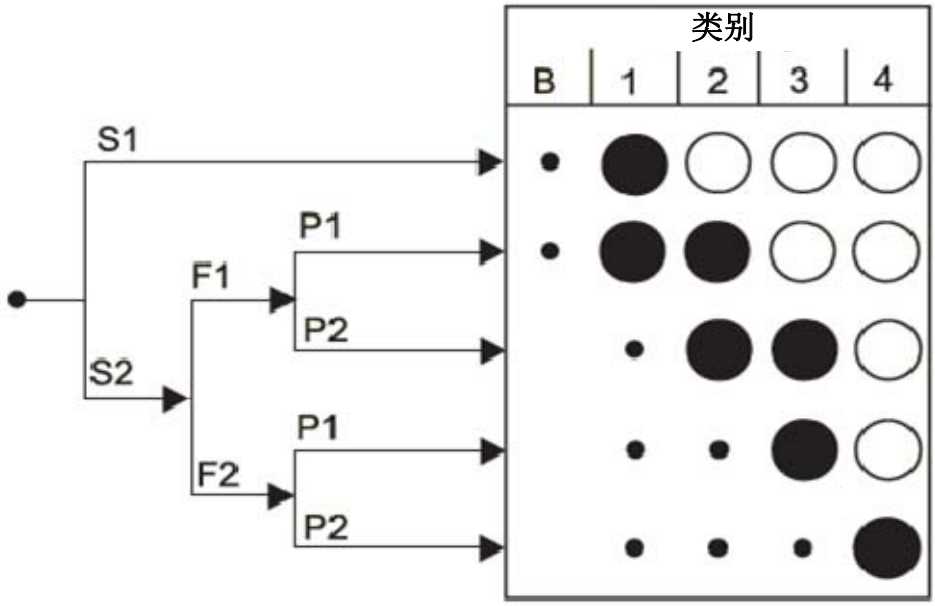
3. 确定避免危害或限制导致的损害的可能性。
   P1 表示在某些情况下可能
   P2 表示几乎不可能

   下图展示了这些步骤：



对安全系统安全类别的说明：

EN 954-1定义了不同风险参数的控制类别。下图展示了如何确定正确的类别：



为控制系统的安全相关零件选择安全类别的方法。EN 954 - 1 标准附录B（资料性）

实心圆圈代表建议的类别。空心圆圈代表超出要求的措施。

EN ISO 13849-1取代了EN 954-1，引入了性能级别（PL）。性能级别考虑了剩余概率。选择的PL应符合IEC EN 61 508规定的安全完整性级别（SIL），还应能够回溯至EN 954-1规定的控制类别。

安全类别决定控制系统的安全相关零件需具备的防故障行为。以下描述了类别B、1、2、3和4。

安全类别B

必须按相关标准设计、建造、选择、组装与合并控制系统的安全相关零件和/或安全设备，以确保这些零件和/或设备耐受：

- 预期的运行应力（例如：与开关容量和开关频率相关的可靠性）
- 使用的材料对作业过程的影响（例如：清洗机中使用的清洗剂）
- 其它相关外部影响（例如：机械振动、外部场、断电或故障）

对于安全类别为 B 类的零件，无需特殊安全措施。故障会导致安全功能丧失。

安全类别1（单通道控制）

必须符合B类要求。必须使用久经考验的部件与安全原理。

故障会导致安全功能丧失，但故障的发生概率小于类别B。

安全类别2（单通道控制与测试）

须满足类别B的要求且须使用久经考验的安全原则。必须通过机器控制系统按适当的间隔测试安全功能。安全功能测试（无论是手动启动的还是自动启动的）必须生成适当控制措施在故障发生时的启动时点。如果不可能实现安全停机，则输出必须提供危险警告。

故障会导致测试间隔内安全功能丧失。安全功能的丧失可通过测试进行检测。

安全类别3（单通道控制（冗余））

须满足类别B的要求且须使用久经考验的安全原则。安全相关零件的设计须满足以下要求：
- 某个安全相关零件发生的单一故障不会导致安全功能丧失
- 可能时，在下次请求安全功能之时或之前检测单一故障

始终在发生单一故障时执行安全功能
- 检测某些而非所有故障
- 未检测到的故障积累到一定程度时会导致安全功能丧失。

安全类别4（单通道控制（冗余）与测试）

须满足类别B的要求且须使用久经考验的安全原则。控制系统的安全相关零件的设计须满足以下要求：
- 某个安全相关零件发生的单一故障不会导致安全功能丧失
- 在下次请求安全功能之时或之前检测单一故障。如果不可能，必须确保故障积累不会导致安全功能丧失。

始终在发生单一故障时执行安全功能。及时检测故障，防止安全功能丧失。

第 5 步：实施功能安全系统：

该步骤中选择用于实施安全功能的硬件。选择的硬件可能包括多个子系统，每个子系统分别有各自的安全性能（SIL 或 PL）。整个安全功能的安全性能与子系统的最低 SIL 或 PL 一样高。

使用未获认证的子系统时，机器制造商须计算每个子系统实现的 SIL 或 PL。EN62061 和 ENISO 13849-1 标准描述了计算过程。这些计算过程复杂，需要的信息可能难以获取。因此，最好使用已获认证的子系统，这类子系统的某些性能级别已计算好。

安全功能的实施包括以下步骤：

1. 按照上一节确定必要的安全性能（SIL 或 PL）。
2. 选择待使用的系统架构。EN ISO13849-1 和 EN62061 提供了基本架构。
3. 用子安全系统（例如：安全装置、开关与继电器等）构造系统。
4. 安装系统时，确保系统的安全完整性不会因接线不当而降低。
5. 验证系统的功能安全性（详见以下章节）。

第 6 步：验证功能安全系统

通过验证功能安全系统证明安全功能的安全性能满足根据风险评估结果制定的要求。

应在实施的同时进行验证。

除验证系统的 SIL 或 PL 外，还须通过功能测试验证安全系统的运行是否正确。

验证安全系统的 SIL （EN 62061）

本指南假设使用的是已获认证的安全子部件。可按照以下步骤验证 SIL。

1. 获取每个子系统的每小时危险失效概率（PFHd）。其应由安全子系统的制造商提供。PFHd 是随机硬件失效值。
2. 对照共因失效（CCF）检查表进行检查，确保考虑了安全系统的所有必要方面。EN 62061 附录 F 提供了该对照表。
3. 按照下表，根据 PFHd 确定子系统的 SIL。

SIL	每小时危险失效概率（1/h）
SIL 1	>= 10-6 且< 10-5
SIL 2	>= 10-7 且< 10-6
SIL 3	>= 10-8 且< 10-7

4. SIL 要求限制 （SILCL）代表子系统的最大 SIL。系统整体的 SILCL 不得高于任何子系统的 SILCL。SILCL 应由安全子系统的制造商提供。

验证安全系统的 PL （EN ISO 13849-1）

本指南假设使用的是已获认证的安全子部件。可按照以下步骤验证 PL。

1. 对照共因失效（CCF）检查表进行检查，确保考虑了安全系统的所有必要方面。EN ISO 13849-1:2008 附录 I 提供了该检查表。

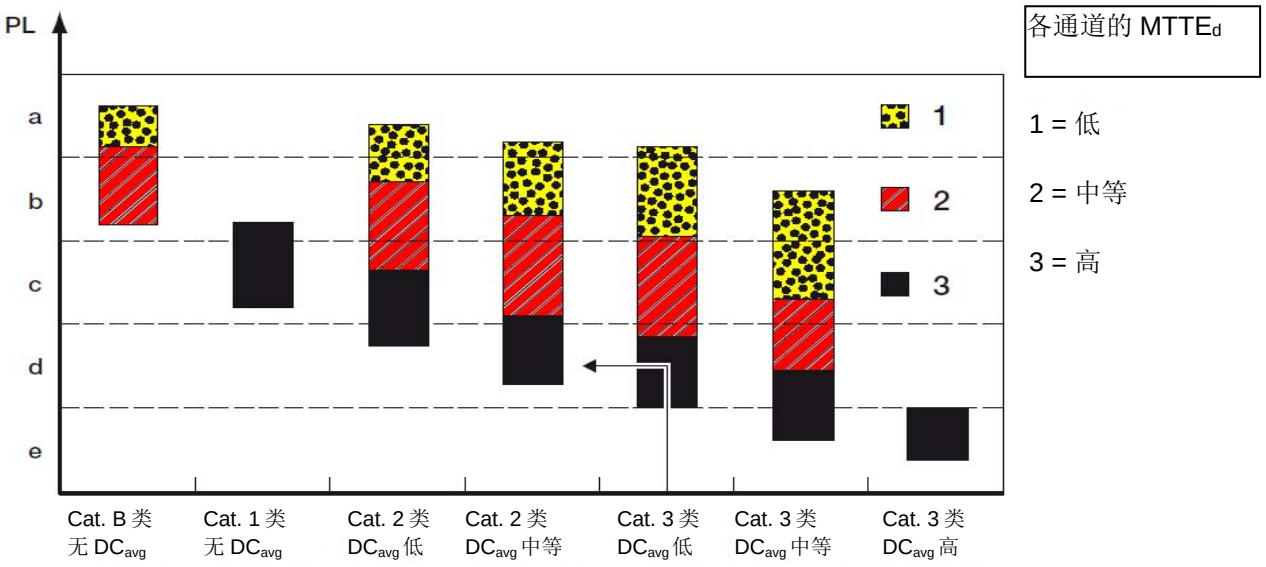
2. 安全子系统的制造商应提供平均危险失效时间（MTTFd），这是危险失效的平均发生时间。下表定性分析了该数值：

质量说明	MTTFd 值范围
低	3 年 <= MTTFd < 10 年
中等	10 年 <= MTTFd < 30 年
高	30 年 <= MTTFd < 100 年

3. 安全子系统的制造商应提供诊断覆盖率（DC），此为可在发生前被诊断到的危险失效。下表定性分析了该数值：

意义	DC 范围
无	DC < 60%
低	60% <= DC < 90%
中等	90 % <= DC < 99 %
高	99% <= DC

4. 在通过风险评估获得 PL 后，可根据下图确定需采取的措施。下图有模棱两可之处。PL 本身涵盖一系列安全措施，因此有选择空间。例如，可以通过 3 种不同的方式实现 PL=d。您可以选择高 MTTFd 与 2 类或低 DC。或者，您也可以选择中等 MTTFd 与较高类别或级别的 DC。



PL 验证示例

SIL 与 PL 的对比

尽管两个标准的评估方法不同，但仍可根据随机硬件失效对比评估结果。

安全完整性级别（SIL）	性能级别（PL）
无对应级别	

第 7 步：确认功能安全系统：

为确保每种安全功能按照风险评估阶段的要求降低风险，须确认每种安全功能。

为确定功能安全系统的有效性，须按照第 2 步中的风险评估过程检验系统。如果系统确实降低了风险，则表示系统有效。

第 8 步：记录功能安全系统

为使机器满足机械指令规定的要求之前，必须记录机器的设计以及提交相关用户文件。

文件需准确且简洁，同时还需向用户提供信息以及易于用户理解。须在用户文件中记录所有剩余风险，并适当说明如何安全地操作机器。文件必须可访问且可维护。用户文件随机器交付。

第 9 步：证明符合性：

在将机器上市销售之前，制造商必须确保机器满足机械指令规定的相关基本健康和安全要求，这种符合性可通过遵循本文件提及的相关协调标准来实现。

有必要提供最新的技术文件来证明符合性，该文件应说明机械的设计、制造与操作。相关更多信息，请参阅 2006/42/EC 指令附录 VII。

为使机器能够在欧盟上市销售，制造商必须随机器提供 EC 符合性声明，在机器上添加 CE 认证标志。

安全停止功能：

几乎所有机器都有停止功能。EN 60204-1针对不同功能要求定义了3类停止功能：

0类停止会导致机器致动机构立即断电。激活电源隔离装置会自动触发0类停止，因为激活隔离装置后，机器无法再获得运动所需的电能。

执行1类停止时，致动机构不断电，以启用受控停止。

2类停止在机器停止后仍需连接电源的情况下使用，因为在受控停止后电源不会断连。

EN 61800-5-2向EN 60204-1列举的停止类别分配了停止功能。EN 61800-5-2将安全功能分为停止功能与其它运动安全功能。如下所示：

安全转矩关闭（STO）

这对应于 0 类停止。电机断电，然后在非受控模式下停止运行。无需监控静止的电机。这通常用作其它某类停止的候补。

安全停止 1（SS1）

这对应于 1 类停止。规定了电机制动方式。在电机静止时执行 STO 功能。驱动内部监控停止功能，缩短停止时间，从而减小与危险的安全距离。

不同的实施方式：

监控延时：非安全驱动技术实施电机减速，在安全监控延时后安全地将驱动与电源断连。

带监控延时的自动静止检测：非安全驱动技术实施电机减速，在安全监控延时后或在安全监控功能检测到电机静止后（以先发生者为准）安全地将驱动与电源断连。

监控制动过程：　　在减速过程中始终通过安全功能监控驱动位置。一旦偏离阈值，会实施 STO。

安全停止 2（SS2）

这对应于 2 类停止。规定了电机制动方式。在电机静止时实施安全操作停止（SOS）。这意味着在电机停止运行后继续实施闭环控制，使电机保持静止。驱动内部监控停止功能，缩短停止时间，从而减小与危险的安全距离。由于驱动仍受闭环控制，因此不会丢失与过程的相对位置，可稍微延迟启动。

不同的实施方式：

监控延时：非安全驱动技术实施电机减速，在安全监控延时后实施 SOS 功能。

带监控延时的自动静止检测：非安全驱动技术实施电机减速，在安全监控延时后或在安全监控功能检测到电机静止后（以先发生者为准）实施 SOS 功能。

监控制动过程：在减速过程中始终通过安全功能监控驱动位置。一旦偏离阈值，会实施 STO。驱动成功达到空转速度和位置后，实施 SOS 功能。

安全运动功能

安全编码器系统：

安全相关监控的实施在很大程度上取决于系统内使用的传感器技术。驱动内使用的传感器技术通常与安全无关，必须加以监控，以防发生故障。下表列举了不同传感器技术的可靠性。

解决方案	描述	安全完整性
标准编码器	用同一透镜评估两信号轨迹	低
两编码器	两个完全独立的通道，成本高昂	很高
一个编码器与一个启动程序	两个完全独立的通道，成本高昂，结果不精确	平均
安全编码器	在同一外壳中安装两个独立的编码器系统，不作安全预处理	高
安全编码器	在同一外壳中安装两个独立的编码器系统，作安全预处理	高
安全编码器	在同一编码器外壳中安装不同的双通道结构	高
标准编码器与电机信号	两个完全独立的不同通道	很高

安全操作停止（SOS）

这意味着在电机停止运行后继续实施闭环控制，使电机保持静止。由于驱动仍受闭环控制，因此不会丢失与过程的相对位置，可稍微延迟启动。

安全限制加速度（SLA）与安全加速度范围（SAR）

Ferraris传感器仅在特殊机器工具或打印机械应用中用于检测加速度。标准驱动无法处理器控制回路中的信号。

安全限制速度（SLS）

该安全功能将电机速度从运行速度降到安全速度，可用于防止预期外的电机启动。一旦电机偏离降低后的速度，通常会实施 SS1 停止功能。

安全速度范围（SSR）

该安全功能用于防止电机速度低于最小值与降低速度，在减速可能导致过程中发生潜在危险事件时使用。当系统中有多个轴时，某个轴突然减速可能会引发危险，因为这可能导致机器受到挤压或其它损坏。
对该错误的响应可能不止使轴停止运动这么简单，至少，可能需使多个轴停止运动。

安全限制转矩（SLT）与转矩安全范围（STR）

由于缺乏合适的传感器技术，因此无法在驱动外部安全地监控电机转矩，但电机转矩与电机电流成比例，因此可间接监控转矩。这意味着需在驱动中集成安全功能以限制扭转矩。

安全限制位置（SLP）

该安全功能用于防止电机运动到位置阈值之外。一旦电机到达位置阈值，需执行某种安全停止功能。电机停止速度的物理限制决定了阈值。该功能要求测量绝对位置。

安全限制增量（SLI）

收到启动命令后，电机可以运动，但不得超过安全限制距离。一旦电机超过安全限制距离，会实施安全停止功能。测量相对位置足以确保该功能正常运行。

安全方向（SDI）

该安全功能防止电机在无效方向上运动，经常与速度限制功能联用。

安全凸轮（SCA）

电机位置在规定的范围内时，该安全功能会触发安全输出信号。该功能要求测量绝对位置。

安全速度监控（SSM）

该功能与安全限制速度（SLS）非常类似，唯一的区别在于不会在速度超出阈值时直接对电机采取措施。该功能仅监控速度并向其它设备发送安全输出信号。

安全制动功能：

安全制动控制（SBC）

该安全功能控制安全输出在电机运动前释放机械制动。制动是“安全制动”，当断电时，会在弹簧弹力的作用下启动。可使用限流电路减少制动释放电磁线圈产生的热量。该功能经常用于起重机以及可能在重力作用下运动的类似负载。

安全制动测试（SBT）

该安全功能使机械制动的保持能力可以在轴静止时被测试。该功能可检测磨损造成的缺陷，向其它系统发送安全输出信号，（例如）使相关区域在问题解决前停止生产。

联系我们

如需更多信息，请联系
您所在地的 ABB 代表或访问以下任一网站：

new.abb.com/motion
new.abb.com/drives
new.abb.com/drivespartners
new.abb.com/PLC